REMARKS / DISCUSSION OF ISSUES

Claims 1-20 are pending in the application. Claim 20 is newly added.

The applicants thank the Examiner for acknowledging the claim for priority and receipt of certified copies of all the priority documents, and for determining that the drawings are acceptable.

The Office action objects to claims 16-19; claims 16 and 19 are rewritten herein in independent form. No new matter is added, and the scope of the claims is unchanged.

The Office action rejects claims 1-19 under 35 U.S.C. 101. The applicants respectfully traverse this rejection.

The Office action notes that claims define nonstatutory processes if they consist solely of mathematical operations without some claimed practical application; or, simply manipulate abstract ideas without some claimed practical application.

The applicants respectfully maintain that the claims do not "consist solely of mathematical operations"; claims 1, 16, and 19 clearly include the steps of sending and receiving data between two parties.

The applicants additionally maintain that the claims are not "without some claimed practical application"; claims 1, 16, and 19 claim a method, system, and program for generating a common secret between a first party and a second party. In the field of communications, there is a practical need for being able to establish a secret (a.k.a. key, code word, etc.) between the authorized parties. As noted in the applicants' specification:

> "Authentication plays an important role in digital communication networks and in content protection systems. Devices that communicate with each other need to be convinced of each other's trustworthiness. They should not give confidential information to a non-trusted party." (Applicants' page 1, lines 14-17.)

And,

> "Basically, one party, called the prover (abbreviated as P) tries to convince another party in the system, called the verifier (abbreviated as V) that he knows a secret that is also known to the verifier. If the verifier is convinced, the prover is authenticated." (Applicant's page 2, lines 13-16.)

The specification includes example practical applications for generating a common secret between parties, including the use of "Chip In Disk" (CID) products that descramble information on a disk only when the receiving device is authenticated.

The applicants also maintain that the claims do not "simply manipulate abstract ideas"; there is nothing 'abstract' about being able to authenticate parties by providing a method, system, and program for generating a common secret between parties.

Because the applicants' claims do not consist solely of mathematical operations, do not simply manipulate abstract ideas, and do provide a practical application, the applicants respectfully maintain that the rejection of claims 1-19 under 35 U.S.C. 101 should be withdrawn.

The Office action rejects claims 1-4, 6, 9-12, 16, 17, and 19 under 35 U.S.C. 102(b) over Matyas et al. (USP 5,953,420, hereinafter Matyas). The applicants respectfully traverse this rejection.

> "A rejection under U.S.C. 102(b) is proper only if ***each and every element*** as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. The ***identical invention*** must be shown in as complete detail as is contained in the claim." **MPEP 2131**. "There must be ***no difference*** between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." **BPAI Opinion No. 2005-2289, October 2005**.

Each of the independent claims 1, 16, and 19 recite calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$, wherein Q(x,y) and P(x,y) are symmetrical polynomials.

Matyas fails to teach calculating a secret as the product of two symmetrical polynomials, as specifically claimed in each of the applicants' independent claims, and thus cannot be said to teach each and every element of the claims as required to support a rejection under 35 U.S.C. 102(b), per MPEP 2131.

The Office action cites Matyas column 6, lines 15-25 for teaching that a first party holds a symmetrical polynomial P(x,y) fixed in the first argument by the value p1. At the cited text, however, Matyas does not reference a symmetrical polynomial, nor a symmetrical polynomial fixed in the first argument by a given value. The term "symmetrical polynomial" is not found anywhere in Matyas.

The Office action also cites Matyas column 7, lines 25-40 for teaching calculating the secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$. At the cited text, however, Matyas does not teach that a secret is determined by the product of two polynomials, as expressly claimed. The Office action acknowledges that Matyas teaches that the secret is calculated in the form of y^x mod p. As is clearly evident, y^x mod p is not equivalent to $Q(q_1, q_2)\cdot P(p_1, p_2)$. As is well known in the art of mathematics, the modulo operation cannot be expressed as a polynomial, and thus Matyas cannot be said to teach forming a secret by multiplying two polynomials, as specifically claimed.

Because Matyas fails to teach calculating a secret S_1 as $S_1=Q(q_1, q_2)\cdot P(p_1, p_2)$, wherein Q(x,y) and P(x,y) are symmetrical polynomials, as specifically claimed in each of the applicants' independent claims, the applicants respectfully maintain that the rejection of claims 1-4, 6, 9-12, 16, 17, and 19 under 35 U.S.C. 102(b) over Matyas is unfounded, per MPEP 2131.

The Office action rejects:

claims 5-8 and 13-15 under 35 U.S.C. 103(a) over Matyas and Menezes et al. (Handbook of Applied Cryptography, hereinafter Menezes); and

claim 18 under 35 U.S.C. 103(a) over Matyas, Menezes, and Oishi (USP 6,298,153). The applicants respectfully traverse these rejections.

> "To establish a *prima facie* case of obviousness … the prior art reference (or references when combined) ***must teach or suggest all the claim limitations***… If the examiner does not produce a *prima facie* case, the applicant is under no obligation to submit evidence of nonobviousness." **MPEP 2142**.

In each of the above rejections, the Office action relies upon Matyas for teaching the elements of claim 1. As detailed above, Matyas fails to teach the elements of claim 1. Accordingly, the applicants respectfully maintain that the

rejections under 35 U.S.C. 103(a) that rely upon Matyas for this teaching are unfounded, per MPEP 2142.

In view of the foregoing, the applicants respectfully request that the Examiner withdraw the rejections of record, allow all the pending claims, and find the application to be in condition for allowance. If any points remain in issue that may best be resolved through a personal or telephonic interview, the Examiner is respectfully requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

/Robert M. McDermott/
Robert M. McDermott, Esq.
Registration Number 41,508
Phone: 804-493-0707
Fax: 215-243-7525

Please direct all correspondence to:
Larry Liberchuk, Esq.
Philips Intellectual Property and Standards
P.O. Box 3001
Briarcliff Manor, NY 10510-8001
Phone: (914) 333-9618
Fax: (914) 332-0615